

Cloudpath

Enrollment System

Release Notes

Software Release 4.3

April 2016

Summary: This document describes the Cloudpath ES release notes for all public releases, including new and updated features, system updates, bug fixes, and known issues. This document includes all release notes for versions 3.0.1914 through the currently released version.

Document Type: Configuration

Audience: Network Administrator



Cloudpath ES Release Notes

Software Release 4.3

April 2016

Copyright © 2016 Ruckus Wireless, Inc. All Rights Reserved.

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ZoneFlex™, BeamFlex™, MediaFlex™, ChannelFly™, and the Ruckus Wireless logo are trademarks of Ruckus Wireless, Inc. All other brands and product names are trademarks of their respective holders.

Copyright © 2016 Ruckus Wireless, Inc. All rights reserved.

Cloudpath ES Release Notes

This document describes the Cloudpath Enrollment System (ES) release notes for all public releases, including new and updated features, system updates, bug fixes, and known issues. This document includes all release notes for versions 3.0.1914 through the currently released version.

Release Notes for Update 4.3.2861

Version 4.3.2861 is a feature release with enhancements, and bug fixes.

This update was released on May 7, 2016.

What to Expect During an Upgrade to Cloudpath ES 4.3

Rebranding from XpressConnect to Cloudpath ES

Product branding has been changed from XpressConnect to Cloudpath ES. In addition to application branding, the executables and log files are also renamed.

Minimum Wizard Version

Because of the branding changes, when upgrading to Cloudpath ES version 4.3, the minimum wizard version must be version 5.0.386 or later, which is the first released Cloudpath-branded wizard.

Snapshots

When upgrading from version 4.2 to 4.3, all previous snapshots will remain in the system, but will be labeled not compatible and will not be selectable for active snapshots. As part of the upgrade process a new snapshot is created with the latest Cloudpath-branded wizard build. This automatic snapshot creation allows the system to be fully updated and usable when the upgrade is finished.

Note >>

Do not reboot the system during the upgrade. The system will reboot itself when the process is complete. Check the update/install logs on the System Updates page for upgrade status.

For more information, see the document, *How to Upgrade Cloudpath ES*, which is located on the Support tab of the Admin UI.

New Features in 4.3.2861

Support for PEAP on Cloudpath ES

Added the ability to support password-based PEAP authentication on the Cloudpath ES. Previously, PEAP/MSCHAPv2 was supported only with the Cloudpath Wizard product. While we still advocate using certificates instead of password for secure onboarding, the new capability for Cloudpath ES provides a migration path for customers using the Wizard product.

To configure a PEAP device configuration, select the Password (PEAP) Authentication style for the WLAN. The device configuration setup wizard prompts you to upload the RADIUS server certificate for an external RADIUS server.

Other credential prompt settings, such as *Display Behavior*, *Username Formatting*, and *Default Credentials* are set from the device configuration *Credentials* tab.

New Wizard for Mac OS X

The generation 2 wizard code, which was previously only available for the Windows OS, is now available for Mac OS X, version 10.8 and later. The new wizard code provides a smaller download package, it does not use Java, and provides improved monitoring of the network state during authentication.

To use the new Mac OS X wizard code, change the *User Experience* settings for the device configuration in your workflow.

Feature Enhancements in 4.3.2861

Updated Account Activation Process

Starting with the Cloudpath ES 4.3 release, new accounts can be created with activation codes, in addition to legacy Cloudpath License Server credentials.

When creating a new account, a Cloudpath License Server administrator adds an activation code to your account. When you log into the hosted server (or log into your on-premise VM), the Cloudpath ES system is tied to your account with the activation code instead of legacy credentials.

Simplified System Setup

The initial system setup for new Cloudpath accounts (cloud or on-premise) has been simplified to reduce errors made during the setup process. The Onboard CA, and the Onboard RADIUS server are setup by default, but can be changed when setup is finished.

The system creates a root and intermediate CA, and the RADIUS server certificate is created using the hostname and given a 5-year expiration.

Authentication Servers

Added support for Internal database users. This Authentication Server option enables end-users to authenticate to accounts defined within this system. This option is not meant to replace AD or LDAP

system in a production environment, but is useful for trial and demo accounts because, with onboard database accounts, there is no need to open firewall ports for testing. It also allows you to create policies based on group information.

Navigate to *Configuration > Advanced > Authentication Servers*, click *Add Server*, and select *Use Onboard Database Server*. To add users, expand the onboard database server in the list and click *Add User*.

Licensing Information

The licensing information now includes system utilization statistics for Users, Authentications, MAC Registrations, Certificates, and Notifications. The links, viewable from the *Support > Licensing* page, add visibility for active concurrent device licensing for guest users.

MAC Registration Enhancements

- MAC Registration Lists can now be sequenced. This is useful because MAC registration filtering is based on first-match.
- To help alleviate common configuration issues with MAC registration, configuration shortcuts have been added for Ruckus Zone Director, Ruckus SmartZone, Cisco, Aruba, and Aerohive controllers.
- Added the ability to filter a workflow split by MAC Registration list.

Certificate Templates

- Added identity options for certificate templates that control whether the certificate's validity is tied to an identity.
 - User + Device - This is the default. The validity of the certificate is based, in part, on the identity of the user (if an identity exists in the enrollment). If the user is blocked, the certificate will be blocked.
 - Device-Only - The validity of the certificate does not take into consideration the identity of the user. If the user is blocked, the certificate will not be affected. With this setting, OCSP does not perform a status check.

RADIUS Attributes

- Added support for the Ruckus Zone Director AP group RADIUS attribute.

Scheduled Reports

- Added server information to reports that have been configured as a scheduled task.

Device Configurations

- Added the ability set up a Ruckus Dynamic PSK device configuration.
- Added the ability to turn Hotspot 2.0 settings on or off for Android devices.

- Moved the Android setting, Trusted Root CA for Web Browsers (Machine), to the CA setting list, allowing it to display the correct UI (which allows the cert to be uploaded).
- Added the ability to add a background color on the AD credential prompt response.
- Added the ability to use a PAC URL to set proxy settings on Android OS version 5.0 and later.
- Added the ability to create a WPA2-PSK WLAN profile.
- Added the ability to disable *Connect to networks shared by my contacts (Wi-Fi Sense)* and *Connect to Suggested Open Hotspots* for Windows 10 devices.

Vouchers

- Added the ability to grant different sponsor permissions for bulk voucher creation. These permissions have been updated for onboard sponsors and for permissions granted in the voucher list.
 - Allow Bulk Creation* controls the ability to create multiple generated vouchers and to upload CSV files.
 - Allow CSV Upload* controls only the ability to upload CSV files.

Cleanup

- Added the ability to Reset Account or Destroy Account. This is useful for when you want to set up an account for demonstration purposes, or if you have an existing hosted account and are moving to an on-premise account. These destroy actions can be accessed from the *Administration > Advanced > Data Cleanup* page.
- Added a script to remove all snapshots. This is useful as part of the process prior to setting up replication. If there are no configuration snapshots on the system, a user attempting an enrollment receives a message that the system is currently disabled.

System Changes in 4.3.2861

PCAP

- Added the ability to grab a packet capture (pcap) file from the Cloudpath ES. From the Linux console, enter **tcpdump**.

Logging

- The syslog configuration now includes JBoss logs.
- Added the ability to set more than one host for where the syslog is sent.

Web Server Certificate

- Added the ability to upload multiple files when uploading a Web Server certificate.

Bugs Fixed in 4.3.2861

- Entering line breaks in the Verification Code Input Message text box no longer cause javascript errors.
- There is no longer a 4096 character limit when adding a custom CA certificate chain.
- The enrollment completes for an Android device set to use the Turkish locale.
- The CURRENT_SERVER_PK no longer remains cached after rebuilding a cluster.
- The SMS Gateways page has been removed from the Cloudpath Admin UI because they are no longer displayed during enrollment.
- When using an SSL port that is not the default, the Sponsorship portal link now displays the updated port.
- When importing the P12 certificate file, a password is always set. The password is derived from (the first matched of) AD/LDAP password, the last 4 digits of the SMS, the voucher, the user's email address, or the assistance ID.
- RADIUS PAP administrator logins are no longer restricted to 16 characters.
- Snapshot creation no longer fails if the referencing device configuration has zero SSIDs or an empty wired configuration.
- If an LDAP authentication server is configured with strip name enabled and username attribute as a non-existent value, and the user enters a domain\username, the enrollment's username variable is correctly set.
- Enrollment records download correctly to an XLS file.
- The /enroll pages will now by default use the output from hostname (in a cluster) rather than the hostname within the enroll URL.
- When configuring the proxy server in ES for iOS devices and Max OS X devices, the port is correctly passed to the device.
- When hostname-restricted is enabled, attempting to connect using an IP address the browser correctly shows a Page Not Found message.
- Using a REST API to get an Enrollment record by MAC address works as expected.
- There is no longer an issue extracting the cab file with running an enrollment on Windows 7/8/10 devices with the non-Unicode language set to Chinese/Japanese.
- The Japan +81 country code has been added to the SMS Country list for Twilio.
- When a voucher is created, the date, time, and timezone are displayed for that voucher. Previously, there was a timezone discrepancy for clients enrolling on hosted systems because it displayed the date in UTC.
- If your configuration includes additional CAs, they are now installed correctly in Android OSes 4.0, 4.1, 4.2, and 4.3.

Release Notes for Update 4.2.2630

Version 4.2.2630 is a maintenance release to address 4.2 migration issues.

This update was released on December 23, 2015.

Bugs Fixed in 4.2.2630

- Fixed an upgrade issue wherein snapshot creation after an upgrade may display an error if a Display Message plug-in is used in the workflow.
- Fixed an issue that caused MAC registration to fail if using a Ruckus SmartZone controller with the *encrypt-mac-ip* setting enabled. This setting in the SmartZone controller must be disabled when integrating with Cloudpath ES.
- The Look & Feel custom background colors now render correctly after the upgrade.
- During initial setup, the system did not check for duplicate administrator email addresses on the company information page. This could cause duplicate administrators to be created in the database, which locked the administrator account and prevented logins.

Release Notes for Update 4.2.2626

This update was released on December 10, 2015.

New Features in 4.2.2626

Administrator Roles

This update adds support for different administrator roles:

- A *CA Administrator* has full configuration and view access to the system.
- An *Administrator* has full configuration and view access to the system, except CA certificates and the private key.
- A *Viewer* has view-only privileges, mostly contained to user, device, or enrollment information. The viewer role has no configuration access and is useful for helpdesk administrators.

Feature Enhancements in 4.2.2626

Additional APIs

The following APIs have been added to the Cloudpath system:

- Register MAC address - Registers the MAC address for the specified device to a specified MAC Registration list.
- Device Capabilities Query - Checks for Hotspot 2.0 capabilities.
- Device Authorization - Authorizes a device on the system.

- Change MAC address - Changes MAC address for an enrollment record.
- Get Device Info by Certificate Serial Number - Queries customer account number for a certificate.
- Get Devices For External ID - Returns all devices associated with a customer account number.
- Get Device Info by MAC address - Queries customer account number for a MAC address.
- Revoke By MAC address and External ID - Revokes one or more certificates associated with a customer account number and specified MAC address.
- Revoke By Certificate Serial Number - Clear Device Capability Cache.
- Destroy Enrollments for External ID - For Testing Only.

OS Settings

- An OS Setting has been added to the Android User Experience, which allows you to suppress the *Rate this App* option. When checked, the *Rate this App* button appears after a successful connection. When unchecked, it does not appear.
- Instructions for manually configuring Windows RT and Windows Phone (8+) are now independently configurable within the Device Configuration.
- Fixed an issue with unmanaged Chrome OS when configuring a “manual” web proxy with a static IP and port.

Workflow Plug-Ins

- Added the ability to set a kill session flag in the *Display Message* workflow plug-in. When set, the session is destroyed when the page is loaded.
- The certificate information for Concurrent Certificates has been enhanced, with the end-user devices sequenced by date issued, listing the oldest enrolled device first.
- For enrollment workflows that do not issue certificates, such as those for MAC registration, you can add an event notification URL to be called based on completion of the workflow.
- Added the ability to enforce a CAPTCHA on the login page for Active Directory and LDAP.
- Added the ability for a branch in the workflow to contain more than 16 options.

Vouchers

- Added the ability for an SMS/email voucher prompt in the workflow to accept vouchers from multiple voucher lists. This, for example, allows a sponsor-created voucher to be submitted on the same screen used for SMS-based authorization.
- Added the ability to use a single voucher code to enroll multiple devices. With this setting, which is controlled in the voucher list, you can specify the number of times a voucher can be reused, or you can suppress this setting for sponsors.

Dashboard

- Added certificate template notifications to the Workflow Information table in the Enrollment record.

- Updated the method for displaying the username in the Enrollments table, to include information gathered from a Data Prompt.
- Added URLs for remote monitoring.
 - /constant/ping.html - tests the web server
 - /admin/ping - tests the application server
 - /enroll/ping - tests the enrollment portal

Certificate Templates

- Added the Start of Half and End of Half settings to the certificate template Start Date and Expiration Dates to allow certificate validity period to be based on a semester schedule.
- Added the ability to include Airespace and Ruckus WISPr VSAs to the RADIUS policy. These VSAs can be added via the certificate template.

System Changes in 4.2.2626

Code-Signing Certificate

- By default, the ES uses the web server certificate as the code-signing certificate to allow iOS devices to display the green “Verified” label, and the System Services page has been updated to reflect this change. A separate code-signing certificate can be uploaded, if desired, but is not normally necessary.

Command-Line Utility

- The restructured the **maintenance scheduled-backup** commands to allow backup via SCP or a mounted (CIFS) drive. New commands include:
 - maintenance scheduled-backup mount setup
 - maintenance scheduled-backup mount remove
 - maintenance scheduled-backup scp setup
 - maintenance scheduled-backup scp remove

Web Server Certificate

- Added the capability to specify one or more Subject Alternative Names (SAN) when generating the CSR for a web server or RADIUS server certificate.

Data Cleanup

- Added the ability to remove old wizard builds and resources on the *Administration > Advanced > Data Cleanup* page.

Bugs Fixed in 4.2.2626

- The system no longer throws an error when the workflow does not capture a username but contains a split with a regex based on username.
- If only the root and intermediate CA are uploaded to a device configuration, and the RADIUS server certificate name is blank, the Connect to Servers flag in the Windows configuration is no longer set by the system.
- If an invalid CSR is detected, the system returns the correct error string.
- The Chrome extension ID for the *XpressConnect Certificate Generator* has been added to the Managed Chromebook Setup Instructions.
- Certificate notifications by 'Specified Date' are correctly sent by the system.
- An error is no longer generated when using the exclamation point character in an SSID name.
- The device configuration description is only visible to administrators and no longer displays to end-users in the profile description.
- The link for the XpressConnect application in the Amazon Appstore has been updated.
- If you include an additional (web) CA in your device configuration, the ONC file for an unmanaged Chromebook shows this CA as trusted.
- Scheduled Reports are now correctly sent by the system. Previously, the scheduler could stop under certain conditions and not process scheduled reports until restarted.
- Documentation links on the *Support > Documentation* page open up in a new tab, rather than in the same window.
- Fixed a thread lock issue that could impact the performance of the system on loads exceeding 450 enrollments per minute for 24 hours.
- Updated the SHA1-to-SHA2 conversion to reuse the serial number by default.
- When Microsoft CA template displays warning that configuration is out of sync, it will not specify the local and remote values.
- Enhanced the upgrade UI and process to provide better feedback on completion status. This will take effect when upgrading from this version.
- Prevent the OCSP accounting threads from shutting down if an exception occurs.
- When reviewing a table of data, the query-by-example lines now support wildcards anywhere, allowing queries like bob@*cloudpath.net.

Release Notes for Update 4.1.2551

This update was released on October 3, 2015

Version 4.1.2551 is a maintenance release to address scheduler issues and issues seen with the iOS 9 and Android 6 operating systems.

Note: This is a critical update for customers that use the onboard RADIUS server.

Bugs Fixed in 4.1.2551

- Fixed an issue where the scheduler can stop functioning causing notifications and scheduled reports to not be sent. With this update, the system will review previously unsent messages and send them if they are less than 7 days old.
- Adds recently released OSes to the ES Admin UI. This includes Mac OS X 10.11, Android 6.0, iOS 9, Fedora 22, and Ubuntu 15.10. These versions were supported in earlier versions using the *Support Future Versions* flag in the device configuration OS settings, but now formally appear in the Admin UI.
- The FreeRADIUS version has been updated to 2.2.8. A known issue in FreeRADIUS version 2.2.6 was causing devices with OSes that use the TLS 1.2 protocol (iOS 9, Android 6) to be unable to associate to a WPA-2 Enterprise/802.1X network, and fail authentication.

Note: If you are using an external RADIUS server and start to see iOS 9 and Android 6 devices fail authentication, you might want to upgrade your RADIUS server.

Release Notes for Update 4.1.2467

This update was released on August 14, 2015

Version 4.1.2467 is a maintenance release to address a few minor issues.

Bugs Fixed in 4.1.2467

- If the NPS generates an OSCP request as a GET, which contains a plus sign (+), this message is correctly decoded by the Apache server. Previously, this resulted in the OCSP Controller getting a value in base64 with a space, causing a base64 parsing exception.
- The process for reparsing User Agents no longer causes the system to timeout during the first login after an upgrade.
- If a workflow *Result* step contains a certificate template, but no network configuration, the user no longer receives an authorization token error. After completing the workflow, the Download Certificate page displays, which allows them to download the p12 certificate.

Release Notes for Update 4.1.2464

This update was released on July 24, 2015

Version 4.1.2464 is a maintenance release, primarily for migration-related bug fixes.

- Customers who have already successfully upgraded to version 4.1.2450 do not need to upgrade to 4.1.2464.
- Customers deploying a new OVA, or upgrading from a version prior to 4.1.2450 via the ES Admin UI, will receive build 4.1.2464.

Migration Issues Fixed in 4.1.2464

- During an upgrade from 2330 to 2450, the upgraded VM no longer receives an exception error when the user attempts to enroll the device. Previously, this occurred if the last snapshot prior to the upgrade was created with Wizard version 5.0.168.
- Fixed an issue where the system stalled on the 4.0.2391 migration script during an upgrade.
- When using a proxy for Android devices, the post-upgrade can successfully create snapshots. Previously, the Android migration script was not properly migrated causing snapshots to fail.
- The snapshot creation process no longer fails with a *no session* error when the default country code in the out-of-band verification plug-in was different from the default country code in the Company Information settings.
- The openssl.cnf file remains on the system with the correct permissions during an upgrade from 4.0.2330 to 4.1.2450. Previously, the absence of this file caused a support file upload to fail.

Bugs Fixed in 4.1.2464

- The ability for a sponsor to create and manage vouchers from the Sponsorship portal has been restored in version 4.1.2464.
- A certificate template notification issued immediately after certificate issuance no longer causes a *no session* error.

Release Notes for Update 4.1.2450

This update was released on July 14, 2015.

Version 4.1.2450 is a feature release with enhancements, bug fixes, and performance improvements.

New Features in 4.1.2450

Send A Notification Plug-in

Added a workflow plug-in that allows a notification to be generated anywhere within the workflow. Notification types include email, SMS, REST API, syslog and more. This step is invisible to the end-user. When utilizing email or SMS, the notification may be sent to the user or to an administrator. All enrollment-related data is available for use in the notification via variables.

Request Access From A Sponsor Plug-In

Added a workflow plug-in to allow guests to request access via sponsorship upon arrival. Whereas the existing sponsorship plug-in requires the sponsor to pre-sponsor the user (by generating a voucher), this new plug-in allows the user to enter their information on a webpage and then request access. The user will be held in a pending state until the sponsor accepts or rejects the request. The request may go to a static user (like a receptionist), to a sponsor selected from a list by the user, or to a sponsor entered by the user.

Generate a Ruckus DPSK Plug-In

Added a workflow plug-in that interacts with Ruckus controllers to generate a Dynamic Pre-shared Key (DPSK). This allows, for example, a gaming system to be registered and issued a unique PSK.

Feature Enhancements in 4.1.2450

New OS Releases

- Added Windows 10 to the UI (was previously *next version*).
- Added Ubuntu 15.04 to the UI (was previously *next version*).

Certificate Templates

- Added the ability to copy a certificate template. Use the copy link on the right side of the certificate template. The copied template may be associated with the same issuing CA or a different issuing CA.
- Added the ability to upload certificates for a template. Use the upload icon on the right side of the certificate template to upload most certificate file formats, either individually or in a zip file. If using P12 files, the files must have a blank password.
- Added a mechanism to enforce the CSR attributes on Chrome OS for a client certificate template issued by a Microsoft Certificate Authority.

Dashboard

- Added the ability to select the columns for scheduled Excel export of enrollment records.
- Added the ability to block all certificates for a user. On the view user page, you can *Revoke/Block All Enrollments*, which treats certificates and MAC registrations as revoked.
- Added an entry to the enrollment record to track the last OCSP request.

Deployment

- Added a WLAN Redirect URL to the Locations page alongside Enrollment Portal and Sponsorship Portal URLs. Use this URL as the redirect URL when defining the system as an external captive portal on a wireless controller. Visually, this is the same as the Enrollment Portal but this URL is more effective at filtering traffic when the controller is redirecting all sorts of traffic, including app traffic, to the enrollment portal.

Device Configuration

- Expanded the Support Next Version flag to be set for each OS family in the device configuration OS settings (rather than globally).
- Added a configuration setting for Android that places the generated device certificate in the certificate store for both the web browser and for Wi-Fi. This is useful when the certificate is used for both Wi-Fi and web-based systems, like web filters.

- Added the ability to hide network configurations that were previously configured in Administrative Console. If you still have legacy configurations in the Administrative Console, we recommend moving to onboard configurations to significantly reduce snapshot time and resource utilization.

Workflow

- When creating a workflow split, you can add a filter based on voucher list. This allows a single prompt for a voucher to diverge based on the voucher list from which the user's voucher originated.
- Added the ability to disable or hide the *Back* button in the workflow.
- Added the ability to hover over settings in the workflow to view the configuration. This includes device configurations, certificate templates, split configuration, and authentication server settings.

Portal

- Updated the portal to only display the download instructions for the user's device. Previously, the page would display a section for each supported OS with the appropriate section expanded. Now, the page will only display the one expanded section. There is a *Show all operating systems* link that will display all available OSes in the event the OS is detected incorrectly.

Support tab

- Restructured the Documentation page to include categories and their associated links and new documents have been added.

Replication

- Added the ability to support internal DNS servers, which is useful in network environments using NAT behind a firewall.

Chromebooks

- Added the ability to remove old certificates in the Certificate Generator extension.
- Added the ability to notify another application when the extension is done installing a client certificate. This is useful when the Enrollment System is part of a larger system initialization application.

Authentication Servers

- Added the ability to completely delete an Authentication Server from the system. Navigate to *Configuration > Advanced > Authentication Servers* and click Edit on the authentication server. In the Cleanup section, use the Delete With Related Data button.
- Added support for wildcards and semi-colon separated lists in the LDAP CN for server certificate validation.

System Services

- Added the ability to configure an SMS gateway using a Twilio account.
- Added System Utilization to the License page, including Active Certificates and Active AD/LDAP Users.

Log Files

- Changed the location on of log files on Windows devices. The new log file location is `%temp%\XpressConnect\XpressConnect.log`, which is normally `C:\Users\<user>\AppData\Local\Temp\XpressConnect\XpressConnect.log`

The preference remains to download the log file from the *Options > Generate Support File* option in the application.

- Updated the system logging on the server to reduce verbosity and provide syslog-parsable formats.

Alpha Release of New Wizard Implementation

- Added a mechanism to test the new Wizard implementation for Windows. By default this is turned off as it has not been vetted for general release. To test this, edit the *User Experience* in the *Device Configuration OS Settings*.

System Changes in 4.1.2450

Licensing

- Added a licensing page (*Support > Licensing*) that provides the status, system utilization, and notices for the current product license.

Database Version

- Upgraded the internal database to MariaDB 5.5.44.

Command-Line Utility

- Added the following new commands to the command-line configuration utility:
 - config ntp-sync-now** - Forces an ntpdate to the configured NTP server.
 - support clean-disk** - The ES runs a clean-disk script on a regular schedule to ensure proper disk space. This command allows an administrator to force it to run.
 - replication force-cleanup** - Forces the removal of the replication setup from the server.

API Updates

- Added the ability to query a mobileconfig file using a REST API call.
- Added the ability to check Hotspot 2.0 capabilities for a device using a REST API call.

Distribution Server DNS and IP Address Change

- Due to performance issues for some global customers, we are moving to an Amazon-based distribution server, which utilizes a new DNS name and IP address. The DNS name is changing from dist.cloudpath.net to dist2.cloudpath.net. The IP address is changing from 72.18.151.79 to 54.226.92.164.

Bugs Fixed in 4.1.2450

- Fixed an issue with the Admin UI that caused it to logout admin sessions despite recent activity. The session now correctly times out 30 minutes after the last use.
- Added a password prompt when downloading a mobileconfig file from the View Certificate page. The password is optional, but if provided, the mobileconfig file will be password-protected.
- Fixed an issue in some Android devices related to Proxy Settings not being applied correctly.
- Changed the Configure link for Android to resolve an issue on Samsung Galaxy S5 devices that prevented the application from launching.
- Added an alternate launch link for Android as a secondary option for devices where the Configure link does not work as expected.
- Resolved an issue with Mac OS X for wired connections using the wizard where the user would be prompted to select the certificate for authentication (after being configured).
- Updated the Managed Chromebook Setup instructions on the *Deploy > Explain Chrome Setup* page.
- Additional details of the RADIUS server certificate can now be viewed on the RADIUS Server configuration page.
- Added the ability to add additional HTTP and HTTPS ports. To date, this is only necessary when using the web redirect capabilities of a Cisco switch for wired 802.1X.
- Fixed an issue with IE 8 that caused it to raise an error when downloading an exe file.
- Fixed an issue with the custom logo in the wizard on Linux OS.
- Corrected the help text related to installing additional CAs.
- Updated the console-based VM setup script to prevent and workaround common user errors.
- Update notification records to include details about skipped notifications.
- Added support for multiple CIDRs to the IP filter restrictions.
- Fixed an issue with the Replace RADIUS Certificate function.
- Added additional checks to prevent incorrect image file types from being uploaded.
- Added `${IDENTITY.FIRST_NAME}` and `${IDENTITY.LAST_NAME}` variables to list of enrollment variables. Previously, the name was only available as a full name.
- Fixed an issue with network configurations defined in the Administrative Console (deprecated) to prevent an Internal Server Error on the download link for Linux devices.
- Added a 'reply-to' address in the email header for new or trial accounts.

- Fixed errors that could occur during a snapshot creation after a multiple version upgrade.
- Corrected the referenced image file type in the page4_javaws.php file.

Test Specifications for Update 4.1.2450

The following details are observations based on upgrade testing. Testing was performed on a Dell R720 (2 CPU x 6 Cores) with the VM assigned 6GB RAM, 2 vCPU x 1 vCore, except for 1M tests which used 12GB RAM, 2 vCPU x 4 vCores. Where singular numbers are provided, the number is the average of the four tests.

TABLE 1. Test Specifications for Update 4.1.2450

Time to Download RPMs	147 seconds
When the download completes, the UI (in 2330) will state that it is <i>Done</i> . [END_OF_STREAM].	
Time to Install Pre-Downloaded RPMs	240 seconds
When the install is complete, the UI (in 2330) will stop adding dots to the progress and the system will reboot.	
Time to Boot, Migrate DB, & Activate Web UI	
This upgrade is sensitive to the number of enrollments in the database.	
50,000 existing enrollments:	133 seconds
250,000 existing enrollments:	455 seconds
500,000 existing enrollments:	947 seconds
1,000,000 existing enrollments:	2077 seconds
The first admin login to the UI will take longer than normal following the upgrade. Some additional one-time data migration will occur during this first login. After boot, the system will continue to migrate enrollment-related data in a throttled background process. The <i>Workflow Information</i> section of the <i>View Enrollment</i> page may lack details for an enrollment until the migration completes. The migration will process the records from newest enrollment to oldest.	
Time to Create Snapshot	
Following the upgrade, a new snapshot should be created for each location. The new snapshot will utilize wizard version 5.0.214 or greater.	
Download new wizard version:	31 seconds
Build snapshot:	19 seconds
Time to Load Issued Enrollments	
50,000 existing enrollments:	1 seconds (previously 1)
250,000 existing enrollments:	3 seconds (previously 6)
500,000 existing enrollments:	5 seconds (previously 25)
1,000,000 existing enrollments:	10 seconds (previously 43)

Release Notes for Update 4.0.2330

This update was released on March 3, 2015.

Version 4.0.2330 is a maintenance release with feature enhancements and bug fixes.

Bugs Fixed in 4.0.2330

- The inline help for the Wizard Logo in the Look and Feel portion of the workflow has been update to include size and file type guidelines.
- If cookies are disabled on the device, the user is directed to enable cookies. Previously, this caused the browser to get stuck in a redirect loop and error out.
- When downloading and importing certificates according to the download instructions for 'Other Operating Systems', the root and intermediate certificates are imported and displayed in the correct order.
- The ES supports the ability to upload non-802.1X certificates, which can be used for web authentication. Upload non-802.1X certificates on the *Device Configurations > Networks tab > Install Additional CAs* section.
- CAs that have been added to the Additional All-OS Configuration for a device configuration are not included in the Linux configuration file, as they are not supported by Linux. The additional CAs are now included in the Android configuration file, as this feature has been added for Android.
- The expiration date displays correctly on the voucher list preview pane if the date in a format of YYYYMMDD.
- Setting up a cluster on an upgraded system no longer causes replication to fail.
- You can use the Android built-in browser for enrollments if cookies are enabled.
- The Email Pattern filter option for a workflow user split is properly evaluated.
- If the serial number for a RADIUS server certificate has one or more leading zeros, the ES formats the serial number to 40 hex characters.

Release Notes for Update 4.0.2325

This update was released on February 13, 2015.

Version 4.0.2325 is a maintenance release with bug fixes.

Bugs Fixed in 4.0.2325

- A sponsor logged in using LDAP group credentials can view and delete unused vouchers.
- When JBoss is stopped and restarted, or shut down using the kill command, extraneous files are cleaned up in the tmp directory.

- Upgrades no longer fail to install the Java binary because of network issues.
- The Enrollment System now provides a mechanism to convert CAs from SHA-1 to SHA-2. Edit the CA and expand the Cleanup section to use this Advanced Option.
- Sponsor logins display the correct message for failed LDAP group authentications.
- The netconfig file for Android accurately reflects the status of the server certificate validation setting.
- The Admin UI inline help link for Variables has been updated to point to the correct location.
- Google authentication configured with anonymous client no longer throws error.
- The timestamp value for MAC registrations now uses the correct format.
- The CA's serial number is converted from decimal to hex when upgrading from versions 2.0.1604 or older.
- The number of characters allowed in the CA Chain field on the Modify Templates page has been increased to prevent the ES from truncating a long CA chain.
- Additional parameters are now included with an internal redirect.
- If you configure an iOS HTTP proxy setting to 'Use automatic proxy configuration URL for this network', this setting is correctly included in the mobileconfig file.
- You receive a warning message in the Admin UI if the Apache server name is not correct.
- A voucher list cannot be deleted if it is used in a workflow.
- The PayloadIdentifier within a mobileconfig file (iOS and Mac OS X) can be modified.
- If an iOS or Mac OS X version is unsupported for a device configuration, the user is unable to download the mobileconfig file and they receive a message that their version is unsupported.
- Extended characters are allowed in the Name, Description, and other labels in the Sponsorship Portal. However, you cannot use an extended character within an OTP. This will cause voucher verification to fail.
- In the /var/log/radius directory, the group radiusd has both read & execute (rx) permissions.
- The icon used in the browser title bar (favicon) can be customized.
- Certificates that expire beyond 2038 no longer cause an incorrect datetime value.
- The Syslog has been expanded to include administration audit information and RADIUS log activity.
- The access log no longer logs credentials when testing the connection to the Microsoft CA using the *Test* button.

Known Issue in 4.0.2325

When importing a database from an older version to a newer release, the timezones must match. For example, the new system cannot have a timezone of MST if the system from which you are importing the database is configured with timezone America/Denver. Use the config timezone command to change the timezone on your system.

Release Notes for Update 4.0.2276

This update was released on December 19, 2014.

Version 4.0.2276 is a maintenance release with bug fixes.

Bugs Fixed in 4.0.2276

- During a sync with the Wizard, old Wizard versions are trimmed and no longer fill up the versions partition.
- When Syslog is configured as UDP, the prefix hostname displays correctly.
- Database records for device cookies are cleared if they do not have a referencing enrollment record.
- Using the Kill Session flag in a Redirect workflow plug-in no longer causes an error or a redirect to a blank page.
- The tar file for the new Java version has been added to the update file to prevent network issues from with Java installation.
- MAC registrations no longer fail to authenticate due to a database query error.
- Scheduled report names now handle the plus sign correctly.
- The httpd file is no longer blank after an upgrade.

Release Notes for Update 4.0.2270

This update was released on December 16, 2014.

Version 4.0.2270 is a feature release with enhancements and bug fixes.

New Features in 4.0.2270

This section describes new features in this release.

New Methods for Onboarding Chromebooks

Added support for automatically distributing user and device certificates to both IT-managed and unmanaged (BYOD) Chromebooks.

- For IT-managed Chromebooks, the Enrollment System (ES) deploys both user and device certificates via a Chrome extension provisioned through the Chromebook management console. Whether tied to the user or the device, the certificates are TPM-backed, which means they are burned into hardware for maximum protection.
- For unmanaged Chromebooks, the ES provides a web portal for self-service and automated installation of the certificate along with configuration of related services, such as WPA2-Enterprise Wi-Fi using EAP-TLS.

Configure Managed or Unmanaged Chromebooks in the *Chrome OS Settings > User Experience* options on the *Configuration > Advanced > Device Configurations* page.

Additionally, the ES provides an Explain Chrome Setup button on the *Configuration > Deploy* page with instructions for setting up Managed Chromebook devices.

HotSpot 2.0 R1

HotSpot 2.0 allows a client device configured with credentials from an authentication provider to automatically connect to a network that supports roaming with the device's home network. When away from the home network, the device queries HotSpot-capable APs to see if the authentication credentials allow it to connect.

In the ES, configure HotSpot 2.0 R1 when you set up your device configuration in the workflow or on the *Configuration > Advanced > Device Configuration > Networks* tab. Choose an SSID Type of use HotSpot 2.0 When Possible. The HotSpot configuration on the device will include the additional HotSpot parameters (Operator, Domain, MMC & MNC, Roaming OI).

The ES supports HotSpot 2.0 R1 for iOS devices, which includes any iOS and greater and Mac OS X Mavericks (10.9) and greater device.

InCommon Certificates

Added support for certificates to be pulled from the InCommon Certificate Services, which is a managed PKI operated by Internet2 and is intended for research and higher education.

Configure the InCommon server information when you create a new certificate template (*Certificate Authority > Manage Templates > Add Template*) and specify that the certificates be pulled from the inCommon certificate service. Your inCommon account information (username, password, web secret key) is required.

eduroam Proxy

Added support in the built-in RADIUS server for eduroam, which allows the authentication requests to be sent to and received from an eduroam RADIUS server. The eduroam federation is the secure, world-wide roaming access service developed for the international research and education community.

Configuration for eduroam is managed from the *Configuration > Advanced > RADIUS Server > eduroam* page. The eduroam configuration supports RADIUS attributes, such as VLAN, Filter ID, and other vendor-specific attributes (VSAs) which can be appended to the RADIUS reply.

Support for SCEP

The ES provides an outward-facing SCEP server interface that allows SCEP clients, such as iOS (via mobileconfig pushed by MDM) to pull certificates via SCEP. The SCEP key is configured for the certificate template (*Certificate Authority > Manage Templates*).

Feature Enhancements in 4.0.2770

This section describes enhancements to existing features.

MAC Registration

Added the ability to upload and pre-enroll MAC addresses for use with MAC-based device authentication. MAC addresses can be imported from the *Configuration > Advanced > MAC Registrations* page.

Vendor-Specific Attributes

Added the ability to append VSAs to RADIUS replies for certificates, MAC registrations, and eduroam authentications. The ES includes all attributes supported by FreeRADIUS plus VSAs for other vendors such as Ruckus. System visibility for each attribute is managed using Show/Hide settings on the *Configuration > Advanced > RADIUS Server > Attributes* page.

RADIUS server

The configuration for the built-in RADIUS server has been moved from System Services to *Configuration > Advanced > RADIUS Server* and includes 5 new tabs: Status, Policy, Clients, eduroam, and Attributes.

- The RADIUS Server Status tab includes all information and processes previously managed in the System Services section.
- The Policy tab includes read-only information about rules applied in the RADIUS server for both WPA2-Enterprise and MAC registration.
- The Clients tab provides the ability to manage RADIUS Clients that are allowed to call into the RADIUS server.
- The eduroam tab allows you to configure the eduroam proxy. To enable the eduroam access server, you must have the IP address, port, and shared secret for the eduroam service.
- The Attributes tab provides the list of RADIUS attributes that are defined in the system. From this tab, you can show or hide which attributes can be selected for certificate templates, MAC registrations, or eduroam configurations.

Configuration Ability for Latest OS Releases

Added independent configuration ability for the latest OS releases, including; Fedora 21, Ubuntu 14.10, Mac 10.10, iOS 8, and Android 5.0. The new OSes are usable on older ES systems, but ES 4.0 allows these OSes to be configured independent of their previous release.

API Enhancements

Added the ability to allow lookup by email and include an optional password for p12 certificates.

Certificates

Added the ability to restrict a certificate template by SSID and include OCSP NameHash and IssuerNameHash to CA information page.

Event Response

Added the ability to allow enrollments to be blocked/unblocked, or to allow certificates to be revoked/unrevoked in batch by uploading a spreadsheet in the *Dashboard > Event Response* page.

Dashboard Tables

The Dashboard tables (Enrollments, Users, Certificates, MAC registrations, and Notifications) have been enhanced to allow export, improved search capabilities, include expired certificates in data export, and to show all date variables in the same format.

Default Templates for Plug-ins

Added the ability to download default templates for any workflow plug-in with the option to upload an HTML template. This includes default templates for the acceptable use policy (AUP), split options, display a message, the credential prompt for local servers, concurrent certificates, vouchers, shared secrets, and out-of-band (OOB) verification for email and SMS.

Data Cleanup

Added the ability to refresh the user agent data when using the Data Cleanup feature (*Administration > Advanced > Data Cleanup*).

Replication

Services that manage replication have been improved; replication logs are sent to a separate file, the process for removing the cluster leaves the servers in a more stable state, and the status graphs have been enhanced.

Sponsorship

Added support for allowing/blocking a sponsor from uploading a bulk voucher list from a spreadsheet.

System Changes in 4.0.2770

This section describes system changes to the Enrollment System.

Apache Hostname

Added the set-apache-servername command to change the Apache server name from the default FQDN. Use the clear-apache-servername to clear a configured apache server name and return it to the FQDN.

Shrink the Database

Added the support shrink-database command to significantly reduce the size of the database file and prevent the system from running out of memory.

Optional Support for SSLv3

Added the config allowapache-sslv3 command to optionally permit the SSLv3 protocol on https connections. The default status of this protocol was changed due to recent SSL vulnerabilities.

Option for Higher Memory Footprints

Added options for higher memory footprints to reduce memory allocation issues.

Updates to Console-Based VM Setup

The console-based VM setup has been enhanced to provide a more comprehensive user experience. The display has been updated, setup questions condensed, and a default hostname was added.

Log Rotate

The log rotate process for RADIUS and Apache logs has been updated to improve disk space issues.

Logging

Added separate settings for SCEP, OCSP, Replication and General logging to allow each to be set in Debug mode without changing the log level of the entire system.

Updated User Agent Parser

Updated the user agent parser to provide more accurate enrollment records.

Bugs Fixed in 4.0.2770

- The download link for the Root CA public key no longer produces an error.
- Ruckus-specific VSAs have been added to the onboard RADIUS server.
- When cleaning up certificate templates, you can choose to either delete issued certificates, or to delete the certificate template along with issued certificates.
- The Chrome OS certificate installation instructions no longer displays the 'Install Your Certificate' instructions twice for the same certificate.
- The Replacement certificate section in the enrollment record no longer shows multiple unrelated user certificates when no MAC address is available.
- The mobileconfig download works correctly when used with Apple's Captive Network Assistant (CNA).
- The Ubuntu user experience correctly matches the device configuration settings.
- MAC Registrations contain the correct attributes when specifying multiple values for the same SSID.

- The logrotate config file has been updated to correctly rotate the RADIUS logs.
- The page4_download instructions for Mac OS X has been updated to correlate with the folder installation process that was implemented for version 2 code-signing.
- The bulk import for vouchers imports all-numeric one-time passwords correctly.
- The MAC registration table supports the ability to search by username.
- Added messaging on Android devices to warn users about using the Firefox browser.
- The bulk import template for sponsorship vouchers now includes the Days of Access field.
- When configured for replication, email notifications sent to the administrator are sent from only one server in the cluster.
- The workflow display for split options has been improved to support a large number of branches.
- The system prevents a web server certificate from being imported as a code-signing certificate and displays an error message.
- The enrollment input fields are encoded to prevent scripting vulnerabilities.
- Scheduled reports with notifications set for Noon and Midnight are sent at the correct time.
- The owner for the RADIUS log is no longer modified during migration.
- The ES correctly handles OCSP GET requests from a Microsoft NPS.
- Processes have been added to better monitor the load balancers in replicated environments.

Release Notes for Update 3.0.2188

This update was released on October 16, 2014.

Version 3.0.2188 is a maintenance release with bug fixes, and includes the updates for the shellshock bash vulnerabilities (CVE-2014-6271 & CVE-2014-7169) for unpatched systems.

Bugs Fixed in 3.0.2188

- Devices running iOS 8 no longer get stuck in a loop when attempting install the network profile.
- The method for signing the application for Mac OS X has been updated to support the new code signatures (version 2) introduced for Mac OS X 10.9.5 (Mavericks). The application continues to support version 1 code-signing for pre-Mavericks OS versions.
- Scheduled Reports configured for 12:00pm are correctly sent at noon.
- The Enrollment System handles OCSP GET requests correctly from Microsoft NPS.
- The inline help for Wizard (App) Messages has been corrected.

Release Notes for Update 3.0.2131

This update was released on July 31, 2014.

Version 3.0.2131 is a maintenance release with bug fixes and minor enhancements.

Feature Enhancements in 3.0.2131

- Added API documentation for REST APIs on the *Administration > Advanced > API Keys* page.
- The certificate serial number has been added to the Certificates table.
- The RADIUS accounting port has been added to the firewall list.
- When a user encounters a redirect that is mis-configured, they are now prompted to redirect again or start over. Previously, the user was caught in a redirect loop.
- Added vendor-specific attribute (VSA) that matches the *Roles > Group Attribute* on the Ruckus wireless controller.
- Added support for operating systems that have recently released beta versions. This includes iOS 8.0, Mac OS X Yosemite (10.10), and Android "L". Note: Support for Mac OS X 10.10 beta version has been added to the Admin UI. However, there is a known issue with this beta version. Updates for Mac OS X beta will be released in future Wizard updates.

System Changes in 3.0.2131

- Tungsten Replicator has been updated to version 2.2.1.
- Added commands to support a cron job for copying the system database:
 - maintenance setup-backup-cron, which sets up a cron job to copy the system database.
 - maintenance remove-backup-cron, which removes the previously setup cron jobs.
- The diag schema-version command was replaced with the following two commands:
 - support view-schema-version, which lists the status of the database schema version.
 - support reset-schema-version, which clears the error flag in the schema version.

Note: The schema-version commands should only be used when working with the support team.

Bugs Fixed in 3.0.2131

- Added the \${SUMMARY} variable, which can be included in an email notification. The output is a snapshot of the user's devices and when each expires.
- When sending a notification for certificate expiration or revocation, the application checks for a newer certificate, and not sent if a newer certificate is found for a specific MAC address.
- Logging in to the ES Admin UI with the recovery user no longer causes an error.
- When configuring MAC registration, you can add RADIUS attributes to all behavior types.
- When using the Japanese translated Wizard, the text along the top of the Download page is translated.

- Changed how proxy information is included in mobileconfig for Mac OS X. Previously, if no proxy was configured, ProxyType=None was specified. Now, this is only included if the proxy setting is explicitly set to NONE (rather than being undefined).
- The bind credentials are now cleared when perform status check is unchecked for an AD server.
- The preference order for populating the outer identity information has been changed to SAN UPN, then CN, then email.
- The local administrative user is processed before LDAP and AD administrators. Previously, this caused local users to be locked out when there was a pinning error with LDAP or AD server certificate.
- Certificates created in ES versions 3.0.1604 are converted from Base10 to hex-based strings so that they can be stored in the database in the same format as certificates created in newer versions of ES.
- The Call URL field for certificate template notifications has been updated to allow long URLs.
- For Windows if Single Sign-On is enabled, the Max Delay field displays a default and the value of 10 is accepted.
- The issues causing errors when downloading a Scheduled Report have been corrected. In a clustered environment, scheduled reports are only sent from the server on which they were configured, but you can download a report from any server in the cluster.

Known Issue in 3.0.2131

This section describes known issues in this maintenance release.

Upgrade Timezone Issue

If you upgrade by downloading a new OVA and importing the database from an existing system, your new OVA must use the same timezone setting as the existing system. A timezone disparity causes a condition in which the private key of the CA is not decrypted, and the RADIUS server does not start.

To check for this condition:

1. Verify that you can view the private key of the CA. Go to *Certificate Authority > Manage CA > View Private Key*. If the text begins with “[CPN:...”, the value failed to decrypt.
2. Verify that the RADIUS server starts. Go to *Administration > System > System Service > RADIUS Component*. If the RADIUS server is running, the power button on the right side of this page is green. If it is clear, the RADIUS server is not running. Try starting the RADIUS server by clicking the power button.

How to Change the Timezone

If needed, you can change the timezone after the upgrade process is finished. This might be required if you are using the Enrollment System in data centers that are in different time zones.

To change the timezone of the new system after the upgrade, follow these steps:

1. Take a snapshot of the virtual machine.

2. Change the timezone of the system, using config timezone command from the service account to change the timezone. For example:

```
#config timezone GMT
```

3. Run the reprotectData command in the browser.

For example, enter `https://<FQDN hostname>/admin/setup/reprotectData`.

4. Verify that you can view the private key and that the RADIUS server starts.

5. Change the timezone of the system. Use the config timezone command from the service account to change the timezone. For example:

```
#config timezone MDT
```

6. Reboot the system.

7. Verify that you can view the private key and that the RADIUS server starts.

Release Notes for Update 3.0.2079

This update was released on June 19, 2014.

Version 3.0.2079 is a maintenance release with bug fixes and feature enhancements.

Feature Enhancements in 3.0.2079

- Added the Post Transition URL setting to the Enrollment System. Configure this setting from *Administration > Advanced > Device Configurations > Networks* tab.
- When using LDAP authentication servers, added the ability to query LDAP attributes using the bind credentials.
- Added the ability to delete a device configuration.
- Added the current version number to the lower left corner of the ES Admin UI.
- Added a check status URL for OCSP to allow a load balancer to query the status of the OCSP service. The URL `http:<admin_svr>/ocsp/ping` should return HTTP 200 with a Success response.
- Added the ability to export an external RADIUS package. The package includes onboard CA certificates, which can be used to set up an external RADIUS server. Download this information from the *Administrator > System > System Services > RADIUS Component*.
- RPM packages are now signed.

Bugs Fixed in 3.0.2079

- The ES yum repository has been updated in response to OpenSSL CVE-2014-0224. This patch can be applied to the ES yum repository from the command line, for all versions of ES (2.x and 3.x), or from the ES Admin UI, in versions 3.0.2050, or later.

Update from the command line, as root:

```
[root@<AccountName> <service account>]#sudo yum clean all
[root@<AccountName> <service account>]#sudo yum update openssl
```

To verify that you have the latest version, run:

```
[root@<AccountName> <service account>]#yum info openssl
```

- The Linux tarball that gets downloaded has the application set to executable.
- The ES now supports SMS messaging outside of the U.S. The +01 Country Code is no longer automatically appended to SMS requests.
- Users can successfully authenticate using Facebook. Previously, the Facebook OAuth API returned an error if the username was included in the data request.
- Added OAuth 2.0 support for Google authentication. Current OAuth Google support was OAuth 1.0a, which has been deprecated by Google. Existing applications should be supported by Google, but we encourage customers to migrate to OAuth 2.0.
- The Allowed IP addresses settings are now properly applied.
- New installations of Win 8.1 (first boot) on a device no longer detect WiFi as wired.
- The Wizard screens have been streamlined for installing multiple networks.
- The Subject Alternative Name (SAN) has been removed from Android log file.
- The <identity> tag is now correctly listed in the Microsoft CA integration.
- You can now upload the private key of a CA that has been generated from a Microsoft CA in the .pfx format.
- When you change the order of plug-ins in a workflow that contains a split, the branch information remains with the correct split.

Replication Issues Fixed

- When one server in the cluster becomes inoperable, the remaining servers in the cluster continue to replicate.
- During an upgrade, the ES verifies that the ES server is bound to the license server before performing a database import.
- During replication setup, the ES allows DNS to resolve to different IP addresses on the servers in the cluster. This is typically needed when two data centers are using network address translation (NAT).
- If the ES detects a failure in a server in the cluster, the server changes to an Offline:Error state. The server is in an error state and will try to correct the issue. This can take 5 to 10 minutes. If the server is unable to resolve the issue, replication should be disabled for troubleshooting.
- The replication configuration can be removed, if needed, even when replication is not running. Go to *Administration > Advanced > Replication* and click the *Remove Cluster* button.

Release Notes for Update 3.0.2050

This update was released on May 22, 2014.

Version 3.0.2050 is a maintenance release with bug fixes and feature enhancements.

Feature Enhancements in 3.0.2050

- Added support for uploading PEM-formatted PKCS#7 certificates.
- Added CSS support for multiple layers of splits in the workflow.
- Enhanced memory management for replication.

Bugs Fixed in 3.0.2050

- The MAC address for Android devices is correctly reported in enrollment record.
- Running the configure proxy setting from the command line correctly sets the configuration file.
- There are no longer memory issues when deploying a large number of enrollment workflows.
- The enrollment table no longer shows an OCSP count when the value is 0.
- Reduced the number of logs generated during OVA download.

Release Notes for Update 3.0.2040

This update was released on April 07, 2014.

Version 3.0.2040 is a maintenance release with bug fixes and feature enhancements.

Feature Enhancements in 3.0.2040

Replication

The Replication user interface has been enhanced to allow you to enable/disable individual servers in the cluster, or to remove the cluster configuration.

When the RADIUS server is restarted on one server in the cluster, this process is replicated to the other RADIUS servers in the cluster.

Operating System Settings

- Settings for PMK caching have been added to the Windows OS Settings.
- The Enrollment System now supports these Motorola scanners:
 - Motorola MC9090 running Windows Mobile 5.0
 - Motorola MC9190 running Windows Mobile 6.0

Certificates

- Active certificates report include non-enrollment-based certificates.
- Expanded variable support for certificate template notifications. To view the list of supported variables for an enrollment, open the enrollment record and scroll down to the Enrollment Variables section.
- Improved the RADIUS and Additional CAs tables on the Device Configuration page to display the certificate trust chain.
- Added the ability to specify Notes for a certificate template, which can be edited from the View Certificates page.
- The certificate upload process has been enhanced to support certificates in a variety of formats (PEM, DER, PFX, PKCS #12, PKCS #7), improve error-checking, and provide a consistent experience throughout the ES, including web server, RADIUS server, and code signing certificates.
- You can upload the root CA with or without the private key, or upload the root CA and remove the private key for enhanced security. When you upload the root or intermediate CA, the ES automatically associates it to the parent/child CA.
- When cloning a certificate template, you can set the CA to sign the new template. The CA and certificate template pages provide more details, including a notification if the private key has been removed.
- OSCP enhancements include improved OCSP caching, a setting in the certificate template to monitor OSCP and allow certificates to be auto-revoked if unseen for a specified number of days, and a change to the OSCP URL to function with the administrative access restriction feature.

Onboard RADIUS Server

- Added the Class attribute to the RADIUS options for a certificate template.
- Enhanced RADIUS logging and debug levels.
- The RADIUS server trust chain, which can be downloaded, is displayed for each device configuration. Go to *Administration > Advanced > Device Configurations > Networks* tab.

Dashboard

The Dashboard has been enhanced to group reporting tables and graphs by function (Enrollments, Certificates, Users & Devices). You can navigate from the User record from the Enrollment table. All Dashboard tables remember the last tab select, filter, and selected page. All tables allow the currently filtered data to be exported to an Excel spreadsheet or downloaded as a CSV file. When exporting data, all columns are included in the exported data, not just the columns displayed.

System Services

- A table of available variables has been added to the enrollment record. The availability of data for each variable is dependent on the enrollment workflow, the data provided by external systems

like Active Directory, and the type of device. This information can be useful for determining which variables to use in certificate notifications.

- Added the ability to upload a support file from the ES Admin UI. Go to *Support > Advanced*.
- Added the ability to clean up the database. You can set thresholds to clean out abandoned enrollments, MAC registrations, certificates, events and notifications. You can destroy certificate authorities, certificate templates, and enrollments, including any child records associated with this data.
- Added the ability to schedule automatic cleanup thresholds from *Administration > Advanced > Data Cleanup*, or you can destroy individual enrollments, certificates, and user records, CAs, and certificate templates and their associated data using the Cleanup section at the bottom of each record.

Enrollments

Enrollments can now be revoked and unrevoked in batch by uploading an Excel spreadsheet that includes the enrollment record information. Go to *Dashboard > Event Response*.

Administrators

You can now select a specific timezone and date format for an administrator location to allow records and events to display in the timezone local to the administrator.

Workflow

Added administrator control over the MAC registration behavior. Additional settings include when to prompt or redirect the user during enrollment.

Wizard

- The *Back* button has been added to enrollment pages.
- The Wizard supports Japanese text for ActiveX and Java applet pages.

Authentication Servers

LDAP and Active Directory authentication servers can be configured to verify the user account during subsequent uses of the certificate.

System Changes in 3.0.2040

- The Enrollment System database was upgraded to MariaDB 5.5.37.
- The onboard RADIUS server automatically restarts when you make changes from the Admin UI. RADIUS changes the cause a restart include certificate template modifications (VLAN or FilterID) or resetting the RADIUS shared secret.
- Added the ability to restrict hostnames, via the command line or ES Admin UI, so that requests that do not match the hostname receive an HTTP 404 error. From the CLI, use the config

hostname-restricted true command. From the Admin UI, go to *Administration > System > System Services* and edit the Web Server.

- Added the ability to shut down the virtual appliance via the command line or ES Admin UI. From the CLI, use the system shutdown command. From the Admin UI, go to *Administration > System > System Services > Virtual Machine > Shutdown*.
- Added the ability to monitor CPU information about the virtual appliance. If disk utilization of a partition exceeds 80%, you receive a warning message on the ES Welcome page. If utilization exceeds 90%, an error displays.
- The service account has been updated to display the clish command prompt upon login. Enter the console command to access the Linux shell. From the Linux shell, enter the config command to return to the service account. Enter ? from either prompt to display help information.
- Added the ability to configure the NTP server during OVA deployment.
- The default Host Memory for the ES virtual appliance has been increased to 6GB.
- The OVA file is now a signed download file.

Bugs Fixed in 3.0.2040

- The ES yum repositories have been updated in response to the SSL vulnerability CVE-2014- 0160, or Heartbleed.
- The Cent OS logrotate file no longer causes the ES onboard RADIUS server to shut down at midnight at the end of the month.
- The ES now validates all LDAP information fields and accepts word or a dash (-) in the DN field.
- When you set up certificate notification with a Trigger Date Basis of Immediately, the enrollment variables are displayed correctly in the notification.
- The system logs have been cleaned up to reduce the number of invalid cookie logs.
- When exporting data from the Enrollments table, the resulting CSV file is correctly formatted to match the columns in the table.
- When uploading a CSV file for vouchers, the correct country code is specified.
- Encrypted RADIUS server certificates now upload successfully.
- You no longer receive an error when using the Chrome browser to run the Wizard on an iOS devices. A message displays to use the Safari browser to access the enrollment URL.
- When setting up an authentication server, all regex fields are now validated when the configuration is Saved.
- CAs and associated templates can now be completely removed from the database.
- The ES now supports certificate formats PEM, DER, PFX, PKCS #12, and PKCS #7.
- Table pagination works correctly on the User & Devices subtables (Devices and Enrollments). •On the Concurrent Certificate workflow plug-in, the *Maximum Concurrent Certificate Count* and *Minimum Concurrent Certificate Count* have been restructured so that the value cannot be left blank.

- Certificate imports no longer fail when a CRL exists but an OCSP URL does not.
- When you copy a certificate template, the associated notification settings are also copied.
- When your account on the hosted Enrollment System is updated, the code-signing certificate is retained.
- When attempting to delete an unused voucher from the Sponsorship Portal, you no longer receive an Internal Server Error.
- The certificate revocation process works correctly when notifications are set for Email or SMS.

Release Notes for Update 3.0.1914

This update was released on February 11, 2014.

Version 3.0.1914 was a major feature release with multiple enhancements and bug fixes.

Feature Enhancements in 3.0.1914

This section describes enhancements to existing features.

Reporting

New reports provide detailed information about the number and status of enrollments on your network by operating systems, device type, and certificate usage. Enrollment records can now be viewed online, downloaded, and scheduled. The new tables and graphs deliver a quick view of the activity on your network. Go to *Operational > Reports* and select a report from the tabs across the top of the page.

Clustering

In addition to VMware-based high availability, this version adds native clustering capabilities, which provides high-availability and high-scalability using two or more servers with all servers being available for active use.

Faster System Setup

A new setup wizard guides you through the system setup process and automates the initial configuration of the virtual appliance to get you up and running quickly.

Device Configurations

- Setting up device configurations, a process previously only available from the Administrative Console (license server), may now be completely specified within the Enrollment System. Device configuration in ES encompasses all aspects of network setup, including WLAN configuration, trusted RADIUS server, CAs and certificates, NAC settings, application installs, and user experience preferences. Moving the device configurations from the license server to the Enrollment System reduces snapshot creation time and utilizes less memory.

- End-user device configuration has been restructured to make it easier to fine-tune settings for specific OS versions, updates, and features, including user experience enhancements.
- Support has been added for automatically generating manual configuration instructions for operating systems that were previously not supported, such as Chrome OS, Blackberry, Windows RT, and a generic configuration. These OSes are added within the device configuration and include settings that provide better control over the user experience, including customizable messaging and enrollment instructions, as well as load preferences.
- The ES makes use of the information provided during the initial system setup to provide preconfigured certificate templates, which can be used immediately for client certificates and certificates for the onboard RADIUS server.

Enhancements

- **Look & Feel Customizations** - All look and feel customizations for the Enrollment System, Wizard, and Download page can be configured in one place. A new modern-style template has been added, and the default templates can be downloaded for modification. HTML, images, and CSS override files can be uploaded to further customize your enrollment pages. To use the new Look & Feel customizations, go to *Configuration > Workflow* and select the *Look & Feel* tab.
- **Workflow** - Device configurations and certificate templates can be created and assigned within the enrollment workflow.
- **Vouchers** - The ES can auto-generate multiple vouchers and automatically assign vouchers, and sponsors can now upload using a CSV template.
- **APIs** - New APIs allow external systems to access and control user, device, and certificate information.
- **MAC Registration** - This new workflow step can be added to the enrollment workflow to register the MAC address of the device, which then makes it available for MAC authentication via RADIUS.

License Server

The Administrative Console has been renamed License Server to more accurately reflect its role as the management device for accounts and licenses. Existing accounts may continue to see the Administrative Console labeling.

External Administrator Authentication

Administrators may now log in to the Enrollment System administrator UI using external credentials, including Active Directory, LDAP, and RADIUS. For Active Directory and LDAP, access may be limited by group membership.

Exchange ActiveSync

The Enrollment System supports configuration of ActiveSync for iOS devices with ActiveSync support. ActiveSync supports email synchronization and remote wipe. ActiveSync can be configured for password-based or certificate-based authentication.

RADIUS PAP Authentication

In addition to AD and LDAP, the ES has added support for authentication via RADIUS using PAP. This includes end user, sponsor, and administrator authentication. Multiple instances may be created as needed.

System Changes in 3.0.1914

This section describes system changes to the Enrollment System.

Web Server Operating System Upgrade

The Enrollment System web server operating system was upgraded to CentOS 6.5.

Boot Password

- A boot password is required during the initial system boot of a new OVA. During OVA deployment, you can specify whether to require a password on all system boots.
- Upgrade systems default to not requiring a boot password. To add a boot password, use the following command from the CLI shell:

```
# config bootpassword enable
```

VMware Tools

As part of the initial system setup of a new OVA, you can install VMware Tools from the virtual appliance console. If you would like to add VMware Tools to your existing system, see the virtual appliance configuration guide on the *Support* tab.

Restrict Administrative Access

You can restrict the IP addresses that can be used to access the ES Admin UI. This can be configured during OVA deployment, or using the following commands from the CLI shell:

```
# config admin allow-access
```

```
# config admin restrict-access <IP address/CIDR>
```

Export the Enrollment System Database

You can export the Enrollment System database to a remote server. The export process dumps the Enrollment System database to a zipped tar.gz file, with a time-stamp, and transfers it using SCP to a remote server.

To export the database, log into the service account and enter the following command from the CLI interface:

```
# maintenance export-database [IP address or hostname] [port] [username] [path to file]
```

For example:

```
# maintenance export-database 172.16.4.20 8022 <ServiceAccount> /home/db/backup
```

Enhanced System Logging

Additional logs include daily and historical file integrity logs and checks for rootkits, backdoors, and possible exploits.

Firewall Troubleshooting

A dynamically generated firewall information page, based on the current system configuration, assists in understanding the inbound and outbound traffic of your Enrollment System. Go to *Administration > Advanced > Firewall Requirements* to view the Enrollment System traffic on your system.

RADIUS Secret

The RADIUS shared secret can be automatically generated or specified by administrator.

Bugs Fixed in 3.0.1914

- There is no longer a white screen while waiting for the ES to generate the mobileconfig file.
- The ES now supports special characters in the workflow name, account name, vouchers, and user passwords.
- The ES now supports LDAP authentication server, including LDAPS.
- The Welcome Title customization accepts double byte characters.
- Regex formats are validated when configured in an option filter for a workflow split.
- New variables are available for email notifications to users and administrators. The variables are listed in the inline help for the Certificate Template Notification.
- You can now download a mobileconfig file from the *Certificate Authority > Issued Certificates > View Certificate* page, for mass configuration of devices.
- The ES can create a batch of vouchers for sponsored access.
- Vouchers can be issued from devices running Internet Explorer in Compatibility Mode.
- The ES Admin UI renders correctly on devices running Internet Explorer in Compatibility Mode.
- You can now perform Updates from the ES Admin UI on systems configured to use a proxy server.
- The ES now supports RADIUS authentication via PAP.
- Sponsors can now log in to the ES Admin UI using credentials from AD, LDAP, and RADIUS if the authentication servers have been configured to allow administrator logins.
- Vouchers can now be tied to a username to allow only the intended user to redeem the voucher.

Known Issues in 3.0.1914

- When you edit changes to the User Experience Options for the Android OS using the Chrome browser, the information saves, but you are taken to a blank page with the word 'data' in the address bar. This is a display issue only and does not affect the data. The application behaves as expected using Firefox and Internet Explorer.
- When replication is enabled, only the main server (the one where the replication setup was initiated) sees the status of the cluster. The other servers incorrectly display Status: Stopped on the System Services page.

Additional Documentation

You can find detailed information in the Enrollment System configuration guides, located on the left-menu *Support* tab of the ES Admin UI.